US-CERT Cyber Security Bulletin

SB04-105 ***April 14, 2004***

Information previously published in CyberNotes will now be incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 3 and April 13, 2004. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	**Operating System**	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/ Alerts**	**Common Name**	**Risk***	**Attacks/ Scripts**
1st Class Internet Solutions[1]	Windows	1st Class Mail Server 4.01	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and multiple Cross-Site Scripting vulnerabilities exist, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	1st Class Mail Server Multiple Input Validation Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concept exploits have been published.
Aborior[2]	Windows, Unix	Encore Web Forum	A vulnerability exists in the 'display.cgi' script due to insufficient validation of user-supplied input in the 'file' variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Encore Web Forum Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit script has been published.

[1] SecurityTracker Alert, 1009705, April 8, 2004.
[2] SecurityFocus, April 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe Systems Incorporated[3]	Windows	Photoshop 8.0	A remote Denial of Service vulnerability exists when a malicious user creates HTML that contains references to Adobe Photoshop COM objects.	No workaround or patch available at time of publishing.	Photoshop COM Objects Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Alan Ward[4]	Windows	A-Cart 2.0, A-Cart PRO 2.0	Multiple vulnerabilities exist: a vulnerability exists in the 'catcode' parameter in 'category.asp' due to insufficient verification, which could let a remote malicious user execute arbitrary code; and a vulnerability in the 'deliver.asp' and 'billing.asp' scripts due to insufficient verification, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	A-Cart Multiple Remote Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
All Enthusiast Inc[5]	Windows, Unix	Photopost PHP Pro 3.1-3.3, 4.0, 4.1, 4.6	Multiple vulnerabilities exist: a vulnerability exists due to insufficient verification of certain parameters before being used in an SQL query, which could let a malicious user execute arbitrary code; a Cross-Site Scripting vulnerability exists in the 'showmembers.php' script due to insufficient verification of user-supplied input, which could let a malicious user execute arbitrary HTML or script code; and a vulnerability exists because certain parameters such as photo names, photo descriptions, album names, album descriptions, and others allow URLs to be specified, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Photopost PHP Pro Multiple Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation[6] ***Trustix issues advisory***[7]	**MacOS X 10.x, Unix**	**Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48**	**An input validation vulnerability exists because escape character sequences can be injected into apache log files, which could let a remote malicious user create arbitrary files or execute arbitrary code.**	**Upgrades available at:** **http://httpd.apache.org/download.cgi** **Netwosix** **http://download.netwosix.org/0006/nepote** ***Trustix:*** **http://www.trustix.org/errata/**	**Apache Error Log Escape Sequence Injection** **CVE Name: CAN-2003-0020**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[3] SecurityTracker Alert, 1009675, April 6, 2004.
[4] Secunia Advisory, SA11236, March 30, 2004.
[5] Securiteam, March 30, 2004.
[6] SecurityFocus, March 20, 2004.
[7] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[8, 9] ***Trustix issues advisory[10]***	**MacOS X 10.x, Unix**	**Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48**	**A remote Denial of Service vulnerability exists via a listening socket on a rarely accessed port.**	**Upgrades available at:** **http://httpd.apache.org/download.cgi** **Netwosix** **http://download.netwosix.org/0006/nepote** ***Trustix:*** **http://www.trustix.org/errata/**	**Apache Connection Blocking Denial of Service** **CVE Name: CAN-2004-0174**	**Low**	**Bug discussed in newsgroups and websites.**
AzDG[11]	Windows, Unix	AzDGDatingLite 2.1.1	Cross-Site Scripting vulnerabilities exist in the language variable and the 'view.php' script due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	AzDGDating Lite Cross-Site Scripting Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
BEA Systems, Inc.[12, 13]	Multiple	WebLogic Server and Express 7.0, SP1-SP4	A vulnerability exists due to a failure to properly associate a user's identity when a client attempts to connect multiple times using different client certificates, which could let a malicious user obtain access to another user's identity.	Updates available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_47.00.jsp	WebLogic Server User Identity Failure	Medium	Bug discussed in newsgroups and websites.
BEA Systems, Inc.[14, 15]	Multiple	WebLogic Server and Express 8.1	A vulnerability exists in the 'config.xml' file due to a coding error, which could let a malicious user obtain sensitive information.	Updates available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_50.00.jsp	WebLogic Server Administrator Password Cleartext Storage	Medium	Bug discussed in newsgroups and websites.
Blaxxun technologies GmbH [16]	Windows	Contact 3D	A buffer overflow vulnerability exists in the Blaxxun Contact 3D browser object for Internet Explorer due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Contact 3D Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[8] SecurityFocus, March 19, 2004.

[9] VU#132110, https://www.kb.cert.org/vuls/id/132110.

[10] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.

[11] waraxe-2004-SA#014, April 8, 2004.

[12] BEASecurity Advisory, BEA04-47.00, April 9, 2004.

[13] VU#858990, https://www.kb.cert.org/vuls/id/858990.

[14] BEA Security Advisory, BEA04-50.00, April 12, 2004.

[15] VU#350350, https://www.kb.cert.org/vuls/id/350350.

[16] Bugtraq, April 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CactuSoft [17]	Windows NT 4.0/2000, 2003	Cactu Shop 5.0 5.1	Multiple vulnerabilities exist: an input validation vulnerability exists in the 'strItems' parameter in the 'mailorder.asp' and 'payonline.asp' scripts, which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'strImage.Tag' parameter in the 'populargeimage.asp script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CactuShop Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however a Proof of Concept exploit has been published.
cdp. Source forge.net[18]	Unix	cdp 0.4, 0.33	A buffer overflow vulnerability exists in the 'printTOC()' function due to insufficient bounds checking, which could let a malicious user cause a Denial of Service and execute arbitrary code.	No workaround or patch available at time of publishing.	CDP PrintTOC Function Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Cisco[19] ***Proof of Concept exploit published*** [20]	**Multiple**	**Catalyst 4000 and 5000 images running version 4.5(2) up to 5.5(4) and 5.5(4a); Catalyst 6000 images running version 5.3(1)CSX, up to and including 5.5(4), 5.5(4a)**	**The telnet server that is built into the Catalyst firmware for remote administration contains a memory leak vulnerability that can result in a Denial of Service.**	**Workaround and patch information available at: http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml.**	**Cisco Catalyst Memory Leak Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Proof of Concept exploit script has been published.*** ***Vulnerability has appeared in the press and other public media.***
Cisco Systems[21]	Multiple	Cisco IOS 11.2(11)	An access control bypass vulnerability exists when transmitting TCP packets to target hosts that have both RST and ACK flags set, which could let a remote malicious user bypass access controls.	No workaround or patch available at time of publishing.	Cisco IOS RST-ACK Packet Access Control Bypass	Medium	Bug discussed in newsgroups and websites.

[17] S-Quadra Advisory #2004-03-31, March 31, 2004.
[18] SecurityTracker Alert, 1009606, April 1, 2004.
[19] Cisco Advisory, CI-00.11, December 6, 2000.
[20] SecurityFocus, March 30, 2004.
[21] SecurityFocus, April 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco[22] *Proof of Concept exploit published*[23]	Multiple	Cisco Catalyst 3500 XL	A vulnerability exists in the configuration interface with the webserver, which could let an anonymous malicious user execute arbitrary commands. This could lead to a complete compromise of the host.	Upgrades available at: http://www.cisco.com	Cisco Catalyst Remote Arbitrary Command Execution CVE Name: CVE-2000-0945	High	Bug discussed in newsgroups and websites. *Proof of Concept exploit script has been published.* *Vulnerability has appeared in the press and other public media.*
Cisco[24] *Proof of Concept exploit published*[25]	Multiple	Cisco IOS versions 12.0-12.1	A Denial of Service vulnerability exists that will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled.	Upgrade available at: http://www.cisco.com/	Cisco IOS "?/" HTTP Request Denial of Service CVE Name: CVE-2000-0380	Low	Bug discussed in newsgroups and websites. Exploit has been published. *Proof of Concept exploit script has been published.* *Vulnerability has appeared in the press and other public media.*
Cisco[26] *Proof of Concept exploit published*[27]	Multiple	IOS 11.0, 11.2x, 11.3x, 12.0x	A Denial of Service vulnerability exists if remote administration via HTML interface is enabled.	No workaround or patch available at time of publishing. Temporary workaround: (Securiteam) Turn off management via HTTP with the following configuration: *no IP http server*	Cisco IOS HTTP Denial of Service CVE Name: CVE-2000-0380	Low/ High (High if DDoS best-practices not in place)	Bug discussed in newsgroups and websites. Exploit has been published. *Proof of Concept exploit script has been published.* *Vulnerability has appeared in the press and other public media.*

[22] Defcom Labs Advisory, def-2000-02, October 26, 2000.
[23] SecurityFocus, March 30, 2004.
[24] Cisco Security Advisory, CI-00.09, October 25, 2000.
[25] SecurityFocus, March 30, 2004.
[26] Securiteam, March 2, 2000.
[27] SecurityFocus, March 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[28] ***Upgrade available*** [29]	**Multiple**	**ATA-186**	**A vulnerability exists because HTTP requests that consist of a single character will cause the device to disclose sensitive information and let a remote malicious user bypass administration authentication.**	***Upgrade available at:*** **http://www.cisco.com/pcgi-bin/tablebuild.pl/ata186?psrtdcat20e2**	**ATA-186 HTTP Device Configuration Disclosure & Web Administration Authentication Bypass** **CVE Name: CAN-2002-0769**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published for the HTTP device configuration vulnerability.** **There is no exploit code required for the administration authentication bypass vulnerability.**
Cisco Systems[30] ***Proof of Concept exploit published*** [31]	**Multiple**	**CBOS 2.3.9, 2.3.8, 2.3.7.002, 2.3.7, 2.3.5.015, 2.3.5, 2.3.2, 2.2.1a, 2.2.1, 2.2.0, 2.1.0a, 2.1.0, 2.0.1, 2.3.053, 2.3, 2.4.1, 2.4.2b, 2.4.2ap, 2.4.2, 2.4.3, 2.4.4**	**Three remote Denial of Service vulnerabilities exist when a large packet is sent to the Dynamic Host Configuration Protocol (DHCP) port, when a large packet is sent to the Telnet port, and the TCP/IP stack will consume all memory while processing received packets if the CPE processes a high number of overly large packets.**	**Upgrade available at:** **http://www.cisco.com**	**Cisco Broadband Operating System Remote Denial of Service Vulnerabilities**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.** ***Proof of Concept exploit script has been published.*** ***Vulnerability has appeared in the press and other public media.***
Cisco Systems[32]	Multiple	Cisco 627, 633, 673, 675, 675E, 677, 677I, 678	A remote Denial of Service vulnerability exists when a malicious user submits multiple consecutive HTTP requests to the Web Management Service.	No workaround or patch available at time of publishing.	Cisco 600 Series Router Web Management Service Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[28] Bugtraq, May 9, 2002.
[29] Cisco Security Advisory, 23888, March 29, 2004.
[30] Cisco Security Advisory, May 23, 2002.
[31] SecurityFocus, March 30, 2004.
[32] SecurityFocus, April 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[33] ***Proof of Concept exploit published***[34]	**Multiple**	**IOS 11.3 & later**	**A vulnerability exists with the HTTP server component of Cisco IOS system software, which could let a remote malicious user gain full administrative privileges if local authentication databases are used.**	**For upgrade information see advisory located at:** **http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html**	**Cisco IOS HTTP Configuration Arbitrary Administrative Access** **CVE Name: CVE-2001-0537**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Proof of Concept exploit script has been published.*** ***Vulnerability has appeared in the press and other public media.***
Cisco Systems[35] ***Proof of Concept exploit published***[36]	**Multiple**	**IOS 12.0-12.2**	**A Denial of Service vulnerability exists when a large number of UDP packets are sent to a device running IOS.**	**No workaround or patch available at time of publishing.**	**IOS UDP Denial of Service** **CVE Name: CAN-2001-1097**	**Low**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit script has been published.*** ***Vulnerability has appeared in the press and other public media.***
Cisco Systems[37]	Multiple	IOS 12.2 ZA, SY, SXB, SXA, (17a) SXA, (14)ZA2, (14)ZA, (14)SY	A remote Denial of Service vulnerability exists when processing Internet Key Exchange (IKE) packets.	Updates available at: http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsm.shtml	IOS Malformed IKE Packet Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[33] Cisco Security Advisory, June 27, 2001.
[34] SecurityFocus, March 30, 2004.
[35] Bugtraq, July 25, 2001.
[36] SecurityFocus, March 30, 2004.
[37] Cisco Security Advisory 50430, April 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[38, 39]	Multiple	Hosting Solution Engine 1105 1.7-1.7.3, Wireless Lan Solution Engine 1105 2.0, 2.0.2, 2.5, 1130 2.0.2, 2.0, 2.0.5	A vulnerability exists in the Cisco Wireless LAN Solution Engine (WLSE) and Hosting Solution Engine (HSE) devices because default usernames and passwords are hardcoded, which could let a remote malicious user obtain sensitive information, obtain complete control over a device or cause a Denial of Service.	Updates available at: http://www.cisco.com/pcgi-bin/tablebuild.pl/1105-host-sol	Cisco WLSE/HSE Devices Default Username and Password	Low/ Medium/ **High** **(Low if a DoS; Medium if sensitive information is obtained; and High if system control is obtained)**	Bug discussed in newsgroups and websites. Exploitation of this issue does not require an exploit. Vulnerability has appeared in the press and other public media.
Citrix[40]	Windows	Meta Frame Password Manager 2.0	A vulnerability exists because passwords are stored in unencrypted form in certain situations, which could let a malicious user obtain sensitive information. *Note: This vulnerability exists only if an administrator hasn't configured the agent to point to a central credential store.*	Hotfix available at: http://support.citrix.com/kb/entry.jspa?entryID=4062	MetaFrame Failure To Encrypt Application Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Clam Anti-Virus[41]	Unix	ClamAV 0.51-0.54, 0.60, 0.65, 0.67, 0.68-1, 0.68	A vulnerability exists if a user has configured a 'VirusEvent' directive in the 'clamav.conf' file and the 'Dazuko' module is used, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Clam Anti-Virus ClamAV Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
cPanel, Inc.[42]	Unix	cPanel 9.1.0-R85	Cross-Site Scripting vulnerabilities exist in the 'account,' 'db,' 'login,' 'email,' 'dir,' 'dns,' and 'ip' parameters of 'ignorelist.html,' 'showlog.html,' 'repairdb.html,' 'doaddftp.html,' 'editmsg.html,' 'testfile.html,' 'erredit.html,' 'dnslook.html,' 'del.html,' and 'index.html' scripts due to insufficient validation, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	cPanel Multiple Module Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proof of Concepts exploits have been published.

[38] Cisco Security Advisory, 50400 Rev. 1.4, April 12, 2004.
[39] VU#659228, https://www.kb.cert.org/vuls/id/659228.
[40] Citrix Document ID CTX103662, April 2, 2004
[41] Bugtraq, March 30, 2004.
[42] Bugtraq, March 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DameWare Developmen LLC[43] ***Upgrade now available***[44]	**Windows NT 4.0/2000, XP**	**Mini Remote Control Server 4.1.0.0**	**A vulnerability exists because the encryption key is sent over the network in plain text format, which could let a remote malicious user obtain sensitive information.**	***Upgrade available at:*** **http://www.dameware.com/download/**	**DameWare Mini Remote Control Server Clear Text Encryption Key Disclosure**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
DameWare Development LLC[45] ***Upgrade now available***[46]	**Windows NT 4.0/2000, XP**	**Mini Remote Control Server 4.1.0.0**	**A vulnerability exists due to a weak random bit generator used to generate encryption keys, which could let a remote malicious user obtain sensitive information.**	***Upgrade available at:*** **http://www.dameware.com/download/**	**Mini Remote Control Server Weak Random Key Generation**	**Medium**	**Bug discussed in newsgroups and websites.**
Emule-Project.net[47]	Windows	Emule 0.42 d	A buffer overflow vulnerability exists due to a boundary error within the 'DecodeBase16()' function that is used in the web server and IRC client code for decoding hexadecimal strings, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://umn.dl.sourceforge.net/sourceforge/emule/eMule0.42e-Installer.exe	eMule Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ethereal Group[48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60] ***Advisories issued and exploit script published***[61, 62, 63, 64]	**Windows 95/98/ME/ NT 4.0, Unix**	**Ethereal 0.8.13, 0.8.14, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.2**	**Multiple vulnerabilities exist: Thirteen stack-based buffer overflow vulnerabilities exist in various protocol dissectors (BGP, EIGRP, IGAP, IRDA, NetFlow, PGM, UCP, NetFlow, IrDA, ISUP, and TCAP), which could let a remote malicious user execute arbitrary code; a remote Denial of Service exists when a malicious user submits a carefully-crafted RADIUS packet; a remote Denial of Service vulnerability exits due to a zero length Presentation protocol selector; and a remote Denial of Service vulnerability exist within the handling of malformed color filter files.**	**Upgrades available at:** **http://www.ethereal.com/download.html** ***Conectiva:*** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000835** ***Netwosix:*** **http://download.netwosix.org/0007/nepote** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/** ***RedHat:*** **ftp://updates.redhat.com/9/en/os/**	**Ethereal Multiple Vulnerabilities** **CVE Names: CAN-2004-0176, CAN-2004-0365, CAN-2004-0367**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[43] SecurityFocus, March 23, 2004.
[44] SecurityFocus, March 29, 2004.
[45] Securiteam, March 25, 2004.
[46] SecurityFocus, March 29, 2004.
[47] SecurityTracker Alert, 1009651, April 3, 2004
[48] Ethereal Advisory, enpa-sa-00013, March 22, 2004.
[49] VU#119876, https://www.kb.cert.org/vuls/id/119876.
[50] VU#124454, https://www.kb.cert.org/vuls/id/124454.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Expinion.net[65] *Fix now available*[66]	Windows NT 4.0/2000, XP, 2003	Member Management System 2.1	A vulnerability exists in the 'resend.asp' and 'news_view.asp' scripts due to insufficient validation of user-supplied input in the 'ID' parameter, which could let a remote malicious user execute arbitrary SQL code.	*Expinion.net has released Member Management System 2.2 to address this issue. Please contact the vendor to obtain the fixed version.*	Member Management System ID Parameter SQL Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Expinion.net[67] *Fix now available*[68]	Windows NT 4.0/2000, XP, 2003	Member Management System 2.1	A Cross-Site Scripting vulnerability exists in the 'error.asp' and 'register.asp' scripts due to insufficient sanitization of the 'err' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	*Expinion.net has released Member Management System 2.2 to address these issues. Please contact the vendor to obtain the fixed version.*	Member Management System Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Expinion.net[69] *Fix now available*[70]	Windows NT 4.0/2000, XP, 2003	News Manager Lite 2.5	Vulnerabilities exist in the 'comment_add.asp,' 'search.asp,' 'category_news_headline.asp,' 'more.asp,' 'category_news.asp,' and 'ews_sort.asp' scripts, which could let a remote malicious user execute arbitrary code or obtain administrative access.	*Expinion.net has released News Manager Lite 2.6 to address these issue. Please contact the vendor to obtain the fixed version.*	Expinion.net News Manager Lite Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[51] VU#125156, https://www.kb.cert.org/vuls/id/125156.
[52] VU#433596, https://www.kb.cert.org/vuls/id/433596.
[53] VU#591820, https://www.kb.cert.org/vuls/id/591820.
[54] VU#644886, https://www.kb.cert.org/vuls/id/644886.
[55] VU#659140, https://www.kb.cert.org/vuls/id/659140.
[56] VU#695486, https://www.kb.cert.org/vuls/id/695486.
[57] VU#740188, https://www.kb.cert.org/vuls/id/740188.
[58] VU#792286, https://www.kb.cert.org/vuls/id/792286.
[59] VU#864884, https://www.kb.cert.org/vuls/id/864884.
[60] VU#931588, https://www.kb.cert.org/vuls/id/931588.
[61] Netwosix Linux Security Advisory, LNSA-#2004-0007, March 29, 2004.
[62] Mandrakelinux Security Update Advisory, MDKSA-2004:024, March 31, 2004.
[63] Red Hat Security Advisories RHSA-2004:136-09 & RHSA-2004:137-01, March 30 & 31, 2004.
[64] Conectiva Linux Security Advisory, CLSA-2004:835, March 31, 2004.
[65] SecurityFocus, March 20, 2004.
[66] SecurityFocus, March 31, 2004.
[67] SecurityFocus, March 20, 2004.
[68] SecurityFocus, March 31, 2004.
[69] SecurityFocus, March 20, 2004.
[70] SecurityFocus, March 31, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Floosietek[71]	Windows	FTGate Office 1.2, FTGate Pro 1.2 (1331), 1.2	Multiple vulnerabilities exist: a vulnerability exists in 'inbox/index.fts' due to insufficient validation of the 'folder' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability exists in 'addresses/individual.fts' due to insufficient sanitization of the 'Display name' field, which could let a remote malicious user execute arbitrary HTML or script code; and an information disclosure vulnerability exists when a remote malicious user requests 'inbox/message.fts' directly without any parameters.	No workaround or patch available at time of publishing.	FTGate Mail Server Multiple Input Validation	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proofs of Concept exploits have been published.
FreeBSD[72]	Unix	FreeBSD 5.2 - Release	A vulnerability exists due to an input validation error within the 'setsockopt()' system call when handling certain IPv6 socket options, which cold let a malicious user obtain sensitive information..	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:06/ipv6.patch	FreeBSD IPv6 Socket Options Information Disclosure	Medium	Bug discussed in newsgroups and websites.
F-Secure[73]	Windows	BackWeb 6.31	A vulnerability exists due to an unspecified error in the BackWeb user interface, which could let a malicious user obtain SYSTEM level privileges.	Hotfix available at: ftp://ftp.f-secure.com/support/hotfix/fsbw/BW_631_hotfix.fsfix	BackWeb Local Privilege Escalation	**High**	Bug discussed in newsgroups and websites. Exploits have been published. Vulnerability has appeared in the press and other public media.
fte.sourceforge.net[74]	Unix	fte text editor 0.49.13	Multiple buffer overflow vulnerabilities exist due to boundary errors within the 'vfte' utility when handling certain command line arguments and environment variables, which could let a malicious user cause a Denial of Service or execute arbitrary code with ROOT privileges.	Updates available at: http://security.debian.org/pool/updates/main/f/fte/	FTE Multiple Local Unspecified Buffer Overflow CVE Name: CAN-2003-0648	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[71] Secunia Advisory, SA11286, April 6, 2004.
[72] Secunia Advisory, SA11233, March 30, 2004.
[73] Secunia Advisory, SA11301, April 6, 2004.
[74] Debian Security Advisory, DSA 472-1, April 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GameSpy[75]	Windows	Roger Wilco Dedicated Server (Linux, BSD) 0.26, 0.27, Dedicated Server (Win32) 0.26-0.30 a, Graphical Server 1.4.1 .6 GameSpy Roger Wilco Graphical Server 1.4.1 .5 GameSpy Roger Wilco Graphical Server 1.4.1 .1-1.4.1 .4	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists exist due to a flaw when handling malicious UDP payloads that are destined for the vulnerable server; a vulnerability exists in the audio service when a malformed UDP datagram is submitted, which could let a malicious user cause a Denial of Service; a vulnerability exists because it is possible to transmit audio on an arbitrary channel without joining it first, which could let a malicious user talk on any channel anonymously (even restricted channels); and a vulnerability exists because IP addresses and ports of connected clients are disclosed to a client entering a channel, which could let a malicious user obtain sensitive information.	This software is no longer supported.	Roger Wilco Server Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Exploit script has been published.
Gentoo[76]	Unix	Linux 1.4_rc1-rc3, 1.4	A vulnerability exists due to the insecure creation of a temporary lockfile, which could let a malicious user obtain sensitive information.	Fix available at: www.gentoo.org/proj/en/portage/index.xml	Gentoo Portage Sandbox Insecure Temporary Lockfile Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[77, 78]	Unix	sharutils 4.2.1	A buffer overflow vulnerability exists in the shar' utility due to a failure to properly validate the size of user supplied strings before copying them to a finite buffer, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.openpkg.org/release/2.0/UPD/sharutils-4.2.1-2.0.1.src.rpm **OpenPKG:** ftp.openpkg.org	GNU Sharutils shar Command Line Parsing Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[75] Bugtraq, March 31, 2004.
[76] Gentoo Linux Security Advisory, GLSA 200404-01, April 4, 2004.
[77] Bugtraq, April 6, 2004.
[78] OpenPKG Security Advisory, OpenPKG-SA-2004.011, April 7, 2005.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
HAHT Commerce, Inc. [79]	Windows Unix	HAHTsite Scenario Server 5.1, Patches 1-6	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Windows: ftp://ftp.haht.com/pub/support/fixes/hs51/build91/ox79989_buffer_overrun_fix.zip Solaris: ftp://ftp.haht.com/pub/support/fixes/hs51/build91/ox79989_buffer_overrun_fix_solaris.tar.gz	HAHTsite Scenario Server Project Name Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company [80]	Unix	Open View Operations for HP-UX 7.0, Solaris 7.0, Vantage Point for HP-UX 6.0, Solaris 6.0	A vulnerability exists due to a missing authentication checking, which could let a remote malicious user obtain unauthorized access.	Upgrades available at: http://itrc.hp.com	OpenView Operations/ VantagePoint Remote Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [81] ***HP issues bulletin***[82]	**Windows**	**Web Jetadmin 7.5.2456**	**Multiple vulnerabilities exist: a vulnerability exists because it is possible to upload HTS files using '/plugins/hpjwja/script/devices_update_printer_fw_upload.hts,' which could let a remote malicious user execute arbitrary code; a vulnerability exists in '/plugins/hpjdwm/script/test/setinfo.hts' due to insufficient verification of the 'setinclude' parameter, which could let a remote malicious obtain sensitive information or execute arbitrary code; a vulnerability exists because a remote authenticated malicious user can upload a specially crafted script and execute the script to cause 'hpwebjetd' to crash; and a vulnerability exists because it is possible to inject arbitrary commands that will be executed when the service is restarted.**	***Workaround available at:*** **http://h20000.www2.hp.com/bizsupport/TechSupport** ***Document.jsp?objectID=c00070269***	**Jetadmin Printer Firmware Update Script Arbitrary File Upload Weakness**	**Low/ Medium/ High** **(Low if a DoS; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser. There is no exploit required for the information disclosure vulnerability. Proof of Concept exploit has been published for the remote arbitrary code execution vulnerability.**

[79] PROTEGO Security Advisory #PSA200405, April 2, 2004

[80] HP Security Bulletin, HPSBMA01010, April 6, 2004.

[81] Bugtraq, March 24, 2004.

[82] HP Security Bulletin, HPSBPI01007, March 31, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[83]	Windows	3.1 Agent for Windows	A remote Denial of Service vulnerability exists when a malicious user submits specially crafted data to TCP port 14247 on the target system.	No workaround or patch available at time of publishing.	IBM Director Agent Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
ImgSvr project[84]	Windows, Unix	ImgSvr Picture Web Server 0.4	Several vulnerabilities exist: a vulnerability exists due to an input validation error when parsing HTTP requests, which could let a remote malicious user obtain sensitive information; and a vulnerability exists which could let a remote malicious user retrieve arbitrary files from the web server root directory and any subdirectories.	No workaround or patch available at time of publishing.	IMGSVR Remote Information Disclosures	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
ImgSvr project[85]	Windows, Unix	ImgSvr Picture Web Server 0.4	Multiple vulnerabilities exist: a buffer overflow vulnerability exists due to insufficient validation of the size of user-supplied HTTP requests, which could let a remote malicious user execute arbitrary code; and a Directory Traversal vulnerability exists due to a failure to properly sanitize user-supplied URI data, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	IMGSVR Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Directory Traversal vulnerability; however, a Proof of Concept exploit has been published.
Innerloop Studios[86]	Windows, Unix	Pan Vision I.G.I-2 Covert Strike 1.0, 1.1, 1.2, 1.3	A format string vulnerability exists due to a failure to properly implement a formatted printing function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Pan Vision IGI-2 Covert Strike Remote Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Interchange[87]	Unix	Interchange 4.8.1-4.8.9, 5.0	A vulnerability exists because it is possible to disclose the content of arbitrary variables by requesting them directly in an URL, which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://www.icdevgroup.org/i/dev/download.html **Debian:** http://security.debian.org/pool/updates/main/i/interchange/	Interchange Remote Information Disclosure CVE Name: CAN-2004-0374	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[83] SecurityTracker Alert ID: 1009665, April 5, 2004

[84] Bugtraq, April 1, 2004.

[85] SecurityFocus, April 5, 2004.

[86] SecurityTracker Alert, 1009667, April 5, 2004.

[87] Debian Security Advisory, DSA 471-1, April 2, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Internet Security Systems[88, 89] *Exploit script published*[90]	Windows NT 4.0/2000	Real Secure Network 7.0, XPU 22.11& prior, Server Sensor 7.0 XPU 22.11 & prior, 6.5 for Windows SR 3.10 & prior, Proventia A & G Series XPU 22.11 & prior, M Series XPU 1.9 & prior, Real Secure Desktop 7.0 ebl & prior, 3.6 ecf & prior, Real Secure Guard 3.6 ecf & prior, Real Secure Sentry 3.6 ecf & prior, BlackICE Agent for Server 3.6 ecf & prior, BlackICE PC Protection 3.6 ccf & prior, BlackICE Server Protection 3.6 ccf & prior	A buffer overflow vulnerability exists due to a boundary error in the PAM (Protocol Analyses Module) component within a routine used for monitoring ICQ server responses, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.iss.net/download/	Internet Security Systems Protocol Analysis Module Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability is being actively exploited in the wild. The W32. Witty Worm exploits this issue and it is propagating with a fixed source port of UDP port 4000. The worm appears to be contained in a single UDP datagram. *Exploit script has been published.*

[88] Bugtraq, March 18, 2004.
[89] VU#947254, https://www.kb.cert.org/vuls/id/947254.
[90] SecurityFocus, March 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
JamesOff [91]	Multiple	Quote Engine 1.0, 1.1	A vulnerability exists in various variables due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://prdownloads.sourceforge.net/topicengine/quoteengine-1.2.0.tar.gz?download	QuoteEngine Mult iple Parameter Unspecified SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Kerio Technologies [92]	Windows	Personal Firewall 4.0.6-4.0.10	A remote Denial of Service vulnerability exists due to a failure to handle '%12' and '%13' characters in URLs when web filtering is enabled.	No workaround or patch available at time of publishing.	Kerio Personal Firewall Web Filtering Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
LBL [93, 94]	Unix	tcpdump 3.4 a6, 3.4, 3.5 alpha, 3.5, 3.5.2, 3.6.2 3.6.3, 3.7-3.7.2, 3.8.1	Two vulnerabilities exist: a buffer overflow vulnerability exists in 'print-isakmp.c' due to insufficient validation of user-supplied input in ISAKMP packets, which could let a remote malicious user cause a Denial of Service and possibly allow the execution of arbitrary code; and a vulnerability exists when a remote malicious user submits an ISAKMP Identification payload with a specially crafted payload length value that is less than eight bytes.	Upgrades available at: http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz **Trustix:** ftp://ftp.trustix.org/pub/trustix/updates/	TCPDump ISAKMP Buffer Overflow & ISAKMP Identification Payload Integer Underflow CVE Names: CAN-2004-0183, CAN-2004-0184	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. An exploit script has been published for the ISAKMP Identification Payload vulnerability.
LCDProc [95]	Unix	LCDProc 0.3, 0.4, 0.4.1 -r1, 4.0, 4.1-4.4	Multiple vulnerabilities exist: a buffer overflow vulnerability exists, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'parse_all_client_messages()' Function, which could let a remote malicious user execute arbitrary code; and a buffer overflow and format string vulnerability exists in the 'test_func_func()' function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://lcdproc.omnipotent.net/download/lcdproc-0.4.5.tar.gz	LCDd Multiple Remote Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[91] SecurityFocus, March 31. 2004

[92] Secunia Advisory, SA11331, April 9, 2004.

[93] Rapid7, Inc. Security Advisory, R7-0017, March 30, 2004.

[94] Trustix Secure Linux Security Advisory, TSLSA-2004-0015, March 30, 2004.

[95] Priv8 Security Research - #2004-001, April 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LinBit Technologies[96]	Unix	LINBOX Office server	Multiple vulnerabilities exist: a vulnerability exists because '//admin/user.ph' can be requested without any user authentication, which could let a remote malicious user obtain access to administrative scripts; and a vulnerability exits due to insecure storage of passwords, which could let a malicious user obtain sensitive information.	Patch available at: http://linbox.linbit.at/patches/linbox-sa1.patch	LINBOX Officeserver Remote Authentication Bypass & Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Liu Die Yu[97]	Multiple	WinBlox 6.0	Multiple buffer overflow vulnerabilities exist in the 'My_CreateFileW' function due to insufficient verification of multiple 'sprintf()' operations, which could let a local/remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	WinBlox My_CreateFileW Buffer Overflows	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Macromedia[98]	Windows, MacOS X, Unix	Dream weaver MX 2004, 6.0, 6.1, Ultradev 4.0	A vulnerability exists when the 'Using Driver On Testing Server' or 'Using DSN on Testing Server' settings are configured in the database connections dialog box, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	Workaround available at: http://www.macromedia.com/devnet/security/security_zone/mpsb04-05.html	Dreamweaver Test Scripts	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
McAfee[99]	Windows	FreeScan	A vulnerability exists in the 'GetSpecialFolderLocation()' Method, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	McFreeScan Module System Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
McAfee[100]	Windows	FreeScan	A vulnerability exists in the 'McFreeScan.CoMcFreeScan.1' COM object, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FreeScan CoMcFreeScan Browser Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[96] SEC-CONSULT Security Advisory, March 30, 2004.
[97] SecurityFocus, March 30, 2004.
[98] Macromedia Security Bulletin, MPSB 04-05, April 2, 2004
[99] Bugtraq, April 7, 2004.
[100] Bugtraq, April 7, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[101] **Updated information**[102]	**Windows 95/98/ME/ NT 4.0/2000, XP, 2003**	**Internet Explorer 5.0.1, SP1-SP4, 5.5, preview, SP1&SP2, 6.0, SP1**	**A vulnerability exists when handling 'CHM' files, which could let a remote malicious user execute arbitrary code.** ***Note:It has been reported that this vulnerability is actively being exploited as an infection vector for malicious code that has been temporarily dubbed 'Ibiza.'***	**No workaround or patch available at time of publishing.**	**Internet Explorer CHM File Processing Remote Arbitrary Code Execution** **CVE Name: CAN-2004-0380**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published and this issue is known to be exploited in the wild.**
Microsoft[103]	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP1	A remote Denial of Service vulnerability exists in 'mswebdvd.dll' when a malicious user submits specially crafted parameters for the 'AcceptParentalLevel Change()' function.	No workaround or patch available at time of publishing.	Internet Explorer MSWebDVD Object Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[104]	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP1	A remote Denial of Service vulnerability exists when Internet Explorer attempts to render IFRAME HTML tags that contain an invalid source argument.	No workaround or patch available at time of publishing.	Internet Explorer Remote IFRAME Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[105]	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP1, Outlook 2003, Outlook Express 6.0	A vulnerability exists when an HTML form is created with the submit 'value' property set to a legitimate site and the 'action' property set to the malicious user specified site, which could let a remote malicious user create a spoofed link that will load an arbitrary URL.	No workaround or patch available at time of publishing.	Internet Explorer HTML Form Status Bar Misrepresentation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[106]	Windows 2000, 2003, XP	Share Point Portal Server 2001, SP1-SP2A	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient input validation in three scripts included with the product, which could let a remote malicious user execute arbitrary HTML or script code.	SharePoint Portal Server 2001 Service Pack 3 available at: http://www.microsoft.com/downloads/details.aspx?FamilyId=15677A92-3470-465F-9F63-E621094103E0&displaylang=en	SharePoint Portal Server Cross-Site Scripting CVE Name: CAN-2004-0379	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[101] SecurityFocus, February 12, 2004.
[102] VU#323070, http://www.kb.cert.org/vuls/id/323070.
[103] SecurityTracker Alert, 1009673, April 6, 2004.
[104] Bugtraq, April 7, 2004.
[105] Bugtraq, March 31, 2004.
[106] SecurityTracker Alert, 1009666, April 5, 204.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[107]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Workstation 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, NetMeeting, Windows 98, SE, ME	A vulnerability exists in LSASS, which could let a remote malicious user execute arbitrary code; a DoS vulnerability exists in LSASS when processing LDAP requests; a vulnerability exists in the Microsoft SSL Library when checking message inputs, which could let a remote malicious user execute arbitrary code; a vulnerability exists in Winlogon, which could let a remote malicious user execute arbitrary code; a vulnerability exists when rendering Metafiles, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Help and Support Center' when handling HCP URLs, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the Utility Manager when launching applications, which could let a remote malicious user obtain SYSTEM privileges; a vulnerability exists in Windows task management, which could let a remote malicious user execute arbitrary code; a vulnerability exists when creating entries in the Local Descriptor Table, which could let a malicious user obtain elevated privileges; a vulnerability exists in the H.323 protocol, which could let a malicious user execute arbitrary code; a vulnerability exists in the Virtual DOS Machine subsystem, which could let a malicious user obtain elevated privileges; a DoS vulnerability exists in Negotiate Security Software Provider, which could also let a remote malicious user execute arbitrary code; a DoS vulnerability exists in the SSL library; & a DoS vulnerability exists in the ASN.1 Library, which could also let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx	Microsoft Windows Multiple Vulnerabilities CVE Names: CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2003-0117, CAN-2003-0118, CAN-2003-0119, CAN-2004-0120, CAN-2004-0123	Low/ Medium/ **High** **(Low if a DoS; Medium if elevated privileges obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[107] Microsoft Security Bulletin, MS04-011, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[108]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME	Multiple vulnerabilities exist: a race condition exists in the RPC Runtime Library, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists in the RPCSS service when a malicious user submits a specially crafted message; a Denial of Service vulnerability exists in the CIS and in the RPC over HTTP Proxy components when a forwarded request to a backend system passes through them; and a an information disclosure vulnerability exists due to the way object identities are created, which could let a malicious user cause applications to listen on unexpected ports.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx	Windows RPC/DCOM Multiple Vulnerabilities CVE Names: CAN-2003-0813, CAN-2003-0816, CAN-2003-0807, CAN-2004-0124	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[108] Microsoft Security Bulletin, MS04-012, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[109]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME	A vulnerability exists when processing specially crafted MHTML URLs, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx	Outlook Express MHTML URL Processing Vulnerability CVE Name: CAN-2004-0380	**High**	Bug discussed in newsgroups and websites.

[109] Microsoft Security Bulletin, MS04-013, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[110]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Workstation 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME	A buffer overflow vulnerability exists in the Jet Database Engine (Jet), which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-014.mspx	Jet Database Engine Buffer Overflow CVE Name: CAN-2004-0197	**High**	Bug discussed in newsgroups and websites.
Mollensoft[111]	Windows	Mollensoft FTP Server 3.6.0	A buffer overflow vulnerability exists in the STOR command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mollensoft FTP Server STOR Command Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mondo Soft[112]	Windows 2000/2003	Mondo Search prior to 5.1b	Multiple vulnerabilities exists: an information disclosure vulnerability exists which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'MsmHigh.exe' script when a specially crafted query string is submitted, which could let a remote malicious user use the search engine as a web proxy; and a remote Denial of Service vulnerability exists when a malicious user invokes 'MsmHigh.exe' or 'MsmLink.exe' multiple times.	Upgrades available at: http://www.mondosoft.com/download/default.asp	MondoSearch Multiple Vulnerabilities	Low/ Medium (Medium is sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

[110] Microsoft Security Bulletin, MS04-014, April 13, 2004.
[111] SecurityTracker Alert ID: 1009638, April 2, 2004
[112] SecurityFocus, April 2, 2004

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Monit Project Group[113, 114, 115, 116]	Unix	TildeSlash Monit 3.0-3.2, 4.0, 4.1, 4.1.1, 4.2, 4.3 Beta 2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a basic authentication requests is submitted without a password; a buffer overflow vulnerability exists during basic authentication procedures due to insufficient bounds checking of usernames, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists n due to an off-by-one error within the handling of POST requests, which cold let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz http://www.tildeslash.com/monit/beta/monit-4.3-beta3.tar.gz **Netwosix:** http://download.netwosix.org/0008/nepote	Multiple Monit Administration Interface Remote Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published for the basic authentication buffer overflow vulnerability.
Mozilla[117] ***Redhat releases updated advisory***[118]	**Windows 95/98/ME/ NT 4.0/2000, MacOS, MacOS X, Unix**	**Mozilla Browser 0.8, 0.9.2.1, 0.9.2-0.9.9, 0.9.35, 0.9.48, 1.0, RC1& RC2, 1.0.1, 1.0.2, 1.1-1.5**	**A Cross-Site Scripting vulnerability exists in 'nsDOMClassInfo.cpp' and occurs when a large number of event handlers are used within HTML tags, which could let a remote malicious user execute arbitrary code.**	**The vulnerability has been fixed in versions 1.6b and 1.4.2 available at:** **http://www.mozilla.org/** ***Redhat:*** **http://rhn.redhat.com/errata/RHSA-2004-110.html**	**Mozilla Browser Zombie Document Cross-Site Scripting Vulnerability** **CAN-2004-0191**	**High**	**Bug discussed in newsgroups and websites.**
Multiple Vendors[119]	Windows NT 4.0/2000, Unix	Active state ActivePerl 5.6.1 .630, 5.6.1-5.6.3, 5.7.1-5.7.3, 5.8-5.8.3, 5.9 dev; Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.3	A buffer overflow vulnerability exists in the 'win32_stat()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	**Activestate:** http://public.activestate.com/cgi-bin/	Perl 'win32_stat()' Function Remote Buffer Overflow CVE Name: CAN-2004-0377	**High**	Bug discussed in newsgroups and websites.

[113] Bugtraq, April 5, 2004.

[114] Netwosix Linux Security Advisory #2004-0008, April 6, 2004.

[115] VU#206382, https://www.kb.cert.org/vuls/id/206382.

[116] VU#623854, https://www.kb.cert.org/vuls/id/623854.

[117] SecurityFocus, February 25, 2004

[118] Redhat RHSA-2004:110-20, April 2, 2004

[119] SecurityFocus, April 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [120]	Windows 98/ME/NT 4.0/2000, XP, 2003	Macromedia Flash 7.0.19 .0; Microsoft Internet Explorer 6.0, SP1	A remote Denial of Service vulnerability exists in the 'LoadMovie' function when a malicious user calls the function and loads a flash movie into a non-zero level.	No workaround or patch available at time of publishing.	Internet Explorer Macromedia Flash Player Plug-in Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors [121]	Multiple	Netscape Enterprise Server for NetWare 4/5 3.0.7 a, 4.1.1, 5.0; Novell Netware 5.1, SP4-SP6, 6.0, SP1-SP3	A Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	NetWare Perl Handler Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors [122] ***More advisories issued***[123]	**Windows**	**UUDeview 0.5.19; WinZip WinZip 7.0, 8.0, 8.1 SR-1, 8.1**	**A buffer overflow vulnerability exists due to a boundary error in the MIME parsing routines, which could let a malicious user execute arbitrary code.**	**UUDeview:** **Windows** **http://www.fpx.de/fp/Software/UUDeview/download/uudeview-win32.zip** **Unix** **http://www.fpx.de/fp/Software/UUDeview/download/uudeview-0.5.20.tar.gz** **WinZip:** **http://www.winzip.com/downwzeval.htm** ***OpenPKG:*** **ftp://ftp.openpkg.org/release**	**UUDeview MIME Archive Buffer Overrun**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Multiple Vendors [124, 125]	Unix	Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4_rc1-rc3, 1.4; MPlayer MPlayer 0.90 rc series, 0.90 pre series, 0.90, 0.91, 1.0 pre1	A buffer overflow vulnerability exists in the 'http_build_request()' HTTP header parsing function due to insufficient verification of the 'Location' HTTP header, which could let a remote malicious user execute arbitrary code.	**MPlayer:** http://ftp3.mplayerhq.hu/MPlayer/releases/MPlayer-0.92.1.tar.bz2	MPlayer Remote 'Location' HTTP header, Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[120] SecurityTracker Alert, 1009674, April 6, 2004.
[121] Novell Technical Information Document, TID10091529, March 26, 2004.
[122] iDEFENSE Security Advisory, February 27, 2004.
[123] OpenPKG Security Advisory, OpenPKG-SA-2004.006, March 12, 2004.
[124] Securiteam, March 31, 2004.
[125] VU#723910, https://www.kb.cert.org/vuls/id/723910.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [126, 127]	Multiple	HP Carrier Grade Server cc2300 A6899A, A6898A, cc3300 A6901A, A6900A, cc3310 A9863A, A9862A; Intel Server Management 5.x, Intel Server Control 3.x	A vulnerability exists in certain Intel Server Control and Server Management utilities due to an invalid firmware setting, which could let a malicious user obtain unauthorized access.	Patches available at: ftp://aiedownload.intel.com/df-support/7321/eng/bmclanfix.exe	Intel LAN Management Server Setup Utilities Configuration	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors [128, 129]	Unix	IPsec-Tools, 0.1, 0.2-0.2.4, 0.3, rc1-rc4; KAME Racoon, 20030711	A vulnerability exists due to an error within the 'eay_rsa_verify()' function in 'crypto_openssl.c' which may allow remote malicious holders of valid X.509 certificates to make unauthorized connections to the VPN without being required to be in possession of the corresponding private key.	Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=74601&release_id=228873 **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Racoon IKE Daemon Unauthorized X.509 Certificate Connection CVE Name: CAN-2004-0155	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[126] Intel Action Alert, AA-679-1, April 5, 2004.
[127] HP Security Bulletin, HPSBGN01009, April 7, 2004.
[128] Mandrakelinux Security Update Advisory, MDKSA-2004:027, April 8, 2004.
[129] VU#552398, https://www.kb.cert.org/vuls/id/552398.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[130131, 132, 133, 134, 135] ***More advisories issued***[136, 137]	**Unix**	**tcpdump versions prior to 3.8.1**	**A remote Denial of Service vulnerability exists when a malicious user submits a malformed ISAKMP packet. This could possibly lead to the execution of arbitrary code.**	**Debian:** **http://security.debian.org/pool/updates/main/t/tcpdump/** **Fedora:** **http://download.fedoralegacy.org/redhat/** **Mandrake:** **http://www.mandrakesecure.net/en/advisories/** **RedHat:** **ftp://updates.redhat.com/9/en/os/** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **SuSE:** **ftp://ftp.suse.com/pub/suse/i386/update/** ***Conectiva:*** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000832** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Server/CSSA-2004-008.0/**	**TCPDump ISAKMP Decoding Remote Denial of Service** **CVE Name: CAN-2003-0989**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[130] SUSE Security Announcement, SuSE-SA:2004:002, January 14, 2004.
[131] Red Hat Security Advisory, RHSA-2004:007-01 & RHSA-2004:008-09, January 14 & 27, 2004.
[132] Debian Security Advisory, DSA-425-1, January 27, 2004.
[133] Mandrake Linux Security Update Advisory, MDKSA-2004:008, January 26, 2004.
[134] SGI Security Advisory, 20040103-01-U, January 28, 2003.
[135] Fedora Legacy Update Advisory, FLSA:1222, January 31, 2004.
[136] SCO Security Advisory, CSSA-2004-008.0, March 3, 2004.
[137] Conectiva Linux Security Advisory, CLSA-2004:832, March 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutt.org [138, 139, 140, 141] ***More advisories issued*** [142,143, 144]	**Unix**	**Mutt 1.2 –1, 1.2.5 .1, 1.2.5 –5, 1.2.5 –4, 1.2.5 -12OL, 1.2.5 –12, 1.2.5 –1, 1.2.5, 1.3.12 –1, 1.3.12, 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.3.27, 1.3.28, 1.4 .0, 1.4.1**	**A buffer overflow vulnerability exists when handling some types of e -mail input, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.**	**Upgrade available at:** **ftp://ftp.mutt.org/pub/mutt/mutt-1.4.2i.tar.gz** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/9/en/os** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** **Trustix:** **ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/mutt-1.4.2-1tr.i586.rpm** ***Netwosix:*** **http://www.netwosix.org/adv01.html** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/1.3/UPD/** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Server/CSSA-2004-013.0/RPMS**	**Mutt Remote Buffer Overflow** **CVE Name: CAN-2004-0078**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
Nessus[145]	Windows	Nessus WX 1.4-1.4.4	A vulnerability exists because usernames and passwords are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NessusWX Account Credentials Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Niels Provos[146]	Unix	Systrace 1.1-1.4	A vulnerability exists due to insufficient sanity checks when handling a process that is being traced with ptrace, which could let a malicious application bypass a Systrace policy.	Upgrades available at: http://niels.xtdnet.nl/systrace/usr-systrace-2004-01-26.tar.gz	Systrace Local Policy Bypass	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
NullSoft [147]	Windows	Winamp 2.91, 3.0, 3.1, 5.0 2, 5.0 1	A vulnerability exists due to a boundary error within the "in_mod.dll" plugin when loading Fasttracker 2 (".xm") media files, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.winamp.com/player/	Winamp 'in_mod.dll' Plug-in Remote Code Execution	High	Bug discussed in newsgroups and websites.

[138] Red Hat Security Advisory, RHSA-2004:051-01, February 11, 2004.
[139] Mandrake Linux Security Update Advisory, MDKSA-2004:010, February 11, 2004.
[140] Slackware Security Advisory, SSA:2004-043-01, February 12, 2004.
[141] Trustix Secure Linux Security Advisory, 2004-0006 , February 13, 2004.
[142] OpenPKG Security Advisory, OpenPKG-SA-2004.005, March 9, 2004.
[143] Netwosix Linux Security Advisory, 2004-0001, March 16, 2004.
[144] SCO Security Advisory, CSSA-2004-013.0, March 26, 2004.
[145] SecurityTracker Alert, 1009577, March 29, 2004.
[146] SecurityFocus, March 29, 2004.
[147] NGSSoftware Insight Security Research Advisory #NISR05042004, April 5, 2004

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Open Text Corporation[148]	Windows	Centrinity FirstClass Desktop Client 7.1	A buffer overflow vulnerability exists in the 'PROXYADDR' variable, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FirstClass Desktop Client Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Open Webmail[149]	Unix	Open Webmail 1.7, 1.8, 1.71, 1.81, 1.90, 2.3	A vulnerability exists if 'use_syshomedir' is set to 'no,' or 'create_syshomedir' is set to 'yes,' which could let a malicious user create arbitrary directories..	Upgrades available at: http://freshmeat.net/redir/openwebmail/14610/url_tgz/download	Open WebMail Arbitrary Directory Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBB[150]	Multiple	OpenBB 1.0.6	A vulnerability exists in 'MyHome.php' due to insufficient sanitization of user-supplied URI data, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenBB MyHome.PHP SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Opera Software[151]	Windows, Unix	Opera Web Browser 7.0 3win32	A remote Denial of Service vulnerability exists when Opera attempts to render IFRAME HTML tags that contain an invalid source argument.	No workaround or patch available at time of publishing.	Opera Web Browser Remote IFRAME Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however a Proof of Concept exploit has been published..
Oracle Corporation[152]	Multiple	Single Sign-On	An information disclosure vulnerability exists because a remote malicious user can create HTML that provides a specially crafted 'p_submit_url' value to the single sign-on server.	No workaround or patch available at time of publishing.	Single Sign-On Customized Login Page Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Panda Software[153]	Windows	Active Scan 5.0	A buffer overflow vulnerability exists in the 'ascontrol.dll' due to a boundary error within the 'ReportHebrew' object, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Panda ActiveScan 'ascontrol.dll' Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[148] SecurityTracker Alert, 1009705, April 8, 2004.
[149] Secunia Advisory, SA11334, April 9, 2004.
[150] SecurityFocus, April 5, 2004.
[151] SecurityFocus, April 9, 2004.
[152] Secunia Advisory, SA11251, March 31, 2004.
[153] Secunia Advisory, SA11312, April 7, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHPKIT[154]	Windows, Unix	PHPKIT 1.6 .03	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHPKit Multiple HTML Injection Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PRAGMA ADE[155]	Unix	ConTeXt	A vulnerability exists in the 'textutil.pl' component of due to a flaw when invoked with the '--silent' option, which could let a malicious user modify information or obtain root access.	No workaround or patch available at time of publis hing.	ConTeXt Temporary File Symlink	Medium/ **High** **(High if ROOT access is obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Prozilla[156]	Windows, Unix	Real Estate Web Template	A vulnerability exists in the site template when a user is registering a username, which could let a remote malicious user bypass payment routines.	No workaround or patch available at time of publishing.	Real Estate Payment. Process Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
psyon.org[157]	Multiple	psInclude 1.41	A vulnerability exists in the 'open()' call due to insufficient verification of input passed to the 'template' parameter, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.psyon.org/projects/psinclude/psinclude142.zip	PSInclude 'open()' call Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Rajesh Kumar Mada-manchi[158]	Unix	RSniff 1.0	A remote Denial of Service vulnerability exists when a client repeatedly connects to the RSniff daemon and does not issue the 'AUTHENTICATE' command to log in or simply closes the connection.	No workaround or patch available at time of publishing.	RSniff Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[154] SecurityFocus, March 30, 2004.
[155] SecuriTeam, April 5, 2004
[156] SecurityTracker , 1009592, March 30, 2004.
[157] Secunia Advisory, SA11235, March 30, 2004.
[158] Secunia Advisory, SA11339, April 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Real Networks[159]	Windows 98/ME/NT 4.0/2000, XP, MacOS X, Unix	RealOne Enterprise Desktop 6.0.11.774, RealOne Player 2.0, 6.0.11.872, 6.0.11.868, 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0 for Windows, 8.0 Win32, 8.0 Unix, 8.0 Mac, 10.0 BETA	A buffer overflow vulnerability exists due to a failure to validate string boundaries when coping user-supplied input into finite buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. *Note: Only users of the RealPlayer that have downloaded the specialized R3T plug-in are affected.*	Update available at: http://service.real.com/help/faq/security/040406_r3t/en/	RealOne Player/ RealPlayer Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Royal Institute of Technology[160]	Unix	KTH Heimdal 0.4 a-0.4 e, 0.5-0.5.2, 0.6 .0	A vulnerability exists due to an error in the validation of cross-realm requests, which could let a malicious user impersonate anyone in the cross-realm trust path.	Upgrades available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/ **Debian:** http://security.debian.org/pool/updates/main/h/heimdal/	Heimdal Kerberos Cross-Realm Validation CVE Name: CAN-2004-0371	Medium	Bug discussed in newsgroups and websites.
Scorched 3D[161]	Unix	Scorched 3D 35.0, 36.0, 36.136.2	Multiple vulnerabilities exist: a format string vulnerability exists within a routine for displaying text entered in a chat box, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and several vulnerabilities exist due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.scorched3d.co.uk/	Scorched 3D Server Memory Corruption Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[159] NGSSoftware Insight Security Research Advisory, April 7, 2004.

[160] Debian Security Advisory, DSA 476-1, April 6, 2004.

[161] Secunia Advisory, SA11319, April 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI[162]	Unix	IRIX 6.5.20 m, 6.5.20 f, 6.5.20, 6.5.21 m, 6.5.21 f, 6.5.21, 6.5.22, 6.5.23	A remote Denial of Service vulnerability exists when handling a link failure, when using the 'PORT' mode, and when using the 'ftp_syslog()' function with anonymous FTP.	Patch available at: http://www.sgi.com/support/security/patches.html	IRIX ftpd Multiple Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
shiba-design [163]	Windows, Unix	Nuke Calendar 1.1 .a	Multiple vulnerabilities exist: a vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL commands; a vulnerability exists in the POST request when a specially crafted request is submitted, which could let a remote malicious user execute arbitrary code; and a path disclosure vulnerability exists when a remote malicious user submits a specially crafted request that triggers an error message.	No workaround or patch available at time of publishing.	NukeCalendar Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
st.Alph-onsos [164]	Unix	Cracka-laka 1.0 .8	A remote Denial of Service vulnerability exists due to a failure to handle invalid input sent directly to the listening port.	No workaround or patch available at time of publishing.	Crackalaka IRC Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Stephen Kozik [165]	Unix	Cloister blog 1.2.2	Several vulnerabilities exist: Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of URI parameters, which could let a remote malicious user execute arbitrary HTML or script code; a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'journal_admin.pl' script due to a failure to authenticate usernames during the administration interface, which could let a remote malicious obtain administrative access.	No workaround or patch available at time of publishing.	Cloisterblog Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed or adminis-trative access obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required; however a Proof of Concept exploit has been published for the Directory Traversal vulnerability.

[162] SGI Security Advisory, 20040401-01-P, April 3, 2004.
[163] waraxe-2004-SA#015], April 8, 2004.
[164] Bugtraq, April 9, 2004.
[165] Bugtraq, March 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc.[166]	Unix	Solaris 9.0_x86, 9.0	A vulnerability exists in the Sun Secure Shell Daemon (SSHD) due to a failure to log client IP addresses when connecting to the service, which could let a remote malicious user bypass security.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris Secure Shell Daemon Client Logging	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Microsystems, Inc.[167]	Unix	Sun Cluster 3.0, 3.1	A Denial of Service vulnerability exists due to a race condition within the Sun Cluster Global File System.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Sun Cluster Global File System Denial of Service	Low	Bug discussed in newsgroups and websites.
SuSE[168]	Unix	Linux 8.2, 9.0 x86_64, 9.0	A vulnerability exists due to the insecure creation of temporary files when an update of the system is performed either via YaST or the 'online_update' utility, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	YaST Online Update Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[169]	Windows	Security Check Virus Detection	A remote Denial of Service vulnerability exists in the Symantec Virus Detection Symantec.SymVAFileQuery.1 COM object when a malicious user invokes the object with excessive data.	No workaround or patch available at time of publishing.	Symantec Security Check Virus Detection COM Object Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Washington University[170, 171] ***More advisories issued[172, 173]***	**Unix**	**wu-ftpd 2.4.1, 2.4.2 academ [BETA1-15], academ [BETA-18], 2.4.2 VR16 & VR17, 2.4.2 (beta 18) VR4-VR15, 2.5.0, 2.6.0-2.6.2**	**A vulnerability exists because directory access restrictions imposed by the 'restricted-gid' option can be bypassed, which could let a remote malicious user bypass access restrictions.**	**Debian:** **http://security.debian.org/pool/updates/main/w/wu-ftpd/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-096.html** ***SGI:*** **ftp://patches.sgi.com/support/free/security/patches/ProPack/** ***TurboLinux:*** **ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/**	**WU-FTPD restricted-gid Access Control** **CVE Name: CAN-2004-0148**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[166] Sun(sm) Alert Notification, 57538, April 7, 2004.
[167] Sun(sm) Alert Notification, 57502, April 8, 2004.
[168] SecurityTracker Alert, 1009668, April 5, 2004
[169] SecurityFocus, April 8, 2004.
[170] RedHat Security Advisory, RHSA-2004:096-09, March 8, 2004.
[171] Debian Security Advisory, DSA 457-1, March 9, 2004.
[172] SGI Security Advisory, 20040303-01-U, March 26, 2004.
[173] Turbolinux Security Advisory, TLSA-2004-8, March 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Web Fresh[174]	Unix	Fresh Guest Book 2.0, 2.1, Guest Book MySQL 1.0	A vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Fresh Guest Book HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
WebCT[175]	Windows 2000, 2003, Unix	WebCT Campus Edition 4.1, 4.1.1.5	A Cross Site Scripting vulnerability exists due to insufficient verification of forum messages, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	WebCT Campus Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
XFree86 Project [176] ***Conectiva issues advisory*** [177]	**Unix**	**XFree86 X11R6 4.1 .0, 4.1–12, 4.1–11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3**	**A remote Denial of Service vulnerability exists in the GLX extension and Direct Rendering Infrastructure components due to insufficient bounds checking.**	**Debian:** **http://security.debian.org/pool/updates/main/x/xfree86/** ***Conectiva:*** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000824**	**XFree86 GLX Extension & Direct Rendering Infrastructure Denial of Service** **CVE Names: CAN-2004-0093, CAN-2004-0094**	**Low**	**Bug discussed in newsgroups and websites.**

[174] SecurityFocus, March 29, 2004.
[175] SecurityTracker Alert, 1009591, March 29, 2004.
[176] Debian Security Advisory, DSA 443-1, February 19, 2004.
[177] Conectiva Linux Security Advisory, CLSA-2004:824, March 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
XMLSoft [178, 179, 180, 181, 182, 183, 184, 185] *More advisories issued*[186, 187]	Unix	Libxml2 2.6.0-2.6.5	A buffer overflow vulnerability exists in 'nanoftp.c' and 'nanohttp.c' when parsing overly long URIs, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://xmlsoft.org/ Debian: http://security.debian.org/pool/updates/main/libx/libxml/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Mandrake: http://www.mandrakesecure.net/en/advisories/ Netwosix: http://download.netwosix.org/0004/nepote OpenPKG: ftp://ftp.openpkg.org/release RedHat: ftp://updates.redhat.com/9/en/os/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/ Trustix: http://www.trustix.org/errata/misc/2004/TSL-2004-0010-libxml2.asc.txt *Conectiva:* ftp://atualizacoes.conectiva.com.br/ *Netwosix:* http://www.netwosix.org/adv04.html	Libxml2 Remote URI Parsing Remote Buffer Overflow CVE Name: CAN-2004-0110	High	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

[178] Fedora Update Notification, FEDORA-2004-087, February 26, 2004.
[179] Red Hat Security Advisory, RHSA-2004:091-01, February 26, 2004.
[180] SGI Security Advisory, 20040301-01-U, March 3, 2004.
[181] Debian Security Advisory, DSA 455-1, March 4, 2004.
[182] Netwosix Linux Security Advisory, March 4, 2004.
[183] Mandrakelinux Security Update Advisory, MDKSA-2004:018, March 4, 2004.
[184] OpenPKG Security Advisory, OpenPKG-SA-2004.003, March 5, 2004.
[185] Trustix Secure Linux Security Advisory, TSLSA-2004-0010, March 6, 2004.
[186] Netwosix Linux Security Advisory, March 4, 2004.
[187] Conectiva Linux Security Announcement, CLA-2004:836, March 31, 2004.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 27 and April 8, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 14 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 8, 2004	**symantecVBScriptExploit.txt**	**Exploit for the Symantec Security Check Virus Detection COM Object Remote Denial of Service vulnerability.**
April 7, 2004	**firstclass_desktop_exp.c**	**Script that exploits the FirstClass Desktop Client Local Buffer Overflow vulnerability.**
April 7, 2004	**mcafeeInfDisclosurePOC.txt**	**Proof of Concept exploit for the FreeScan CoMcFreeScan Browser Information Disclosure vulnerability.**
April 6, 2004	**Blaxxun.POC.txt**	**Proof of concept exploit for the Contact 3D Remote Buffer Overflow vulnerability.**
April 5, 2004	**igi2fs.zip**	**Exploit for the Pan Vision IGI-2 Covert Strike Remote Format String vulnerability.**
April 5, 2004	monit4.2_exp.c	Script that exploits the Monit basic authentication buffer overflow vulnerability.
April 3, 2004	**aboriorEncoreWebForumExploit.pl**	**Proof of Concept exploit for the Encore Web Forum Remote Arbitrary Command Execution vulnerability.**
April 1, 2004	ethereal_igap_exp.c	Script that exploits the Ethereal Buffer Overflow vulnerabilities.
March 31, 2004	**wilco2.zip**	**Proof of Concept exploit script for the Roger Wilco Server UDP Datagram Handling Denial Of Service vulnerability.**
March 30, 2004	**ciscoMultipleVulnsExploit.pl**	**Perl script that exploits the Cisco Broadband Operating System Remote Denial of Service Vulnerabilities, Cisco IOS "?/" HTTP Request Denial of Service, Cisco Catalyst Remote Arbitrary Command Execution, Cisco Catalyst Memory Leak Denial of Service, Cisco IOS HTTP Denial of Service, Cisco IOS HTTP Configuration Arbitrary Administrative Access, and IOS UDP Denial of Service vulnerabilities.**
March 30, 2004	tcpdump-isakmp-id-uflow.c	Script that exploits the TCPDump ISAKMP Identification Payload Integer Underflow Vulnerability.
March 29, 2004	557iss_pam_exp.c	Script that exploits the Internet Security Systems Protocol Analysis Module Remote Buffer Overflow vulnerability
March 29, 2004	systrace_exp.c	Script that exploits the Systrace Local Policy Bypass vulnerability.
March 27, 2004	Systrace.txt	Exploit for the Systrace Local Policy Bypass vulnerability.

Trends

- **US-CERT is aware of exploitation of a cross-domain scripting vulnerability in the InfoTech Storage (ITS) protocol handlers used by Microsoft Internet Explorer (IE). By convincing a victim to view an HTML document (web page, HTML email), an attacker could execute arbitrary code with the privileges of the user running IE and read or modify content in another web site. For more information see Internet Explorer CHM File Processing Remote Arbitrary Code Execution entry in Bugs, Holes & Patches table and US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **US-CERT is aware of a new mass-mailing malicious code known as "Sober.F". Sober.F arrives as an email message written in German or English and containing a 42,496-byte email attachment. For more information see W32.Sober.F@mm, (item is boldfaced/red) in the Virus Section below and US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Exploit code has been publicly released that takes advantage of multiple vulnerabilities in various Cisco products. For more information see Cisco Systems entries in the Bugs, Holes & Patches table and US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **There are a number of pieces of malicious code spreading on the Internet through e-mail attachments, peer-to-peer file sharing networks and known software vulnerabilities. Current threats include the Phatbot Trojan Horse, W32/Beagle Virus, W32/Netsky Virus, and the W32/MyDoom Virus. For more information, see Cyber Security Alert SA04-079A located at:** http://www.us-cert.gov/cas/alerts/SA04-079A.html**.**
- **A virus known as the "Witty" worm is spreading over the Internet and has damaged computers worldwide. It exploits the Internet Security Systems Protocol Analysis Module Remote Buffer Overflow vulnerability.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Netsky	Worm	Increase	February 2004
2	W32/Bagle	Worm	Stable	January 2004
3	PE_NIMDA	Worm	Return to table	October 2001
4	W32.Welchia.B	Worm	Return to table	August 2003
5	PE_VALLA	File Infector	New to table	May 2003
6	JAVA_BYTEVER	Java applet	New to table	May 2003
7	PE_PARITE	File Infector	Return to table	January 2001
8	W32/MyDoom	Worm	Decrease	January 2004
9	W32/Sober	Worm	Decrease	December 2003
10	W32/Swen	Worm	Stable	September 2003

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

W32/Agobot-FJ (Aliases: Backdoor.Agobot.iz, W32/Gaobot.worm.gen.d) (Win32 Worm): This is an IRC backdoor Trojan and peer-to-peer (P2P) worm which opens TCP ports to listen for and process commands received from a remote intruder. This worm will move itself into the Windows System32 folder under the filename WINII.EXE and create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Video Poes = winii.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Video Poes = winii.exe

The following registry entries will also be created:

- HKLM\System\CurrentControlSet\Services\Video Poes\
- HKLM\System\CurrentControlSet\Enum\Root\Legacy_Video_Poes\

W32/Agobot-FJ will attempt to terminate anti-virus and software firewall processes, in addition to other viruses, worms or Trojans. This worm will search for shared folders on the internet with weak passwords and copy itself into them. W32/Agobot-FJ can sniff HTTP, VULN, FTP and IRC network traffic and steal data from them. This worm can also exploit the DCOM vulnerability on unpatched systems and manipulate registry keys. This worm will attempt to test the available bandwidth by posting data to the following sites:

- www.st.lib.keio.ac.jp
- www.lib.nthu.edu.tw
- www.stanford.edu
- www.xo.net
- www.utwente.nl
- www.schlund.net

W32/Agobot-FJ can also be used to initiate denial-of-service (DoS) and synflood/httpflood/udpflood attacks against remote systems. This worm can redirect TCP and GRE data and steal the Windows Product ID and keys from several computer games.

W32.Antinny.K (Win32 Worm): This is a variant of W32.HLLW.Antinny.G that spreads using the Winny file-sharing network and steal personal information.

W32.Blackmal.B@mm (Alias: W32/MyWife.a@MM, I-Worm.Nyxem, W32/Nyxem-A, WORM_BLUEWORM.A) (W32 Worm): This worm is a minor variant of W32.Blackmal@mm. The two differ only in the size of the worm, some possible viral file names, and e-mail subjects and messages that the worm creates. The major viral behaviors of both variants are identical. This threat is written in the Microsoft Visual Basic language and is compressed with UPX.

W32.Bugbear.E@mm (Alias: PWS.Hooker.Trojan, W32/Bugbear.C.worm) (W32 Worm): This variant of W32.Bugbear@mm spreads as an e-mail attachment and steals information from the infected computer. The malformed e-mail from the worm uses the Microsoft Internet Explorer Unspecified CHM File Processing Arbitrary Code Execution Vulnerability (CAN-2004-0380) in Internet Explorer to run a malicious program. The worm is written in Microsoft Visual C++ and packed with UPX.

W32.Gaobot.SY (Win32 Worm): This is a worm that attempts to spread through network shares that have weak passwords and allows malicious user to access an infected computer using a predetermined IRC channel. The worm uses mu ltiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 80. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043)
- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 machines using this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434.
- Sending itself to the backdoor port, which the Beagle family of worms opens.
- Sending itself to the backdoor port, which the Mydoom family of worms opens.

W32.Gaobot.UJ (Win32 Worm): This is a variant of W32.Gaobot.gen. It attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.

It is packed first with ASPack, and then with Morphine.

W32.Gaobot.UL (Win32 Worm): This is a variant of W32.Gaobot.gen. It attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer through a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.

It is packed with PE Diminisher.

W32.Gaobot.UM (W32 Worm): This variant of W32.Gaobot.gen attempts to spread through network shares that have weak passwords. It also allows malicious users to access an infected computer through a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.

W32.Gaobot.UM is packed with ASPack.

W32.Gaobot.WX (W32 Worm): This worm attempts to spread through network shares with weak passwords and allows malicious users to access an infected computer through IRC. The worm uses multiple vulnerabilities to spread, including:

- Weak passwords
- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

W32.HLLP.Philis (Win32 Virus): This is a virus that prepends itself to .exe files and attempts to steal passwords for the game, Legend of Mir 2.

W32.Lovgate.R@mm (Alias: W32/Lovgate.x@MM, I-Worm.LovGate.w) (Win32 Worm): This variant of W32.Lovgate@mm is a mass-mailing worm that attempts to e-mail itself to all the e-mail addresses it finds on the computer. The worm has the following characteristics:

- Drops a backdoor component.
- Attempts to copy itself to poorly secured remote shares, scanning contiguous IP ranges, seeking accessible IPC$ or ADMIN$ shares.
  Such copies of the worm may be enticingly named, or within ZIP or RAR archives. The worm carries a list of typical username/password combinations which it uses in attempting to get write access to remote shares
- If it is able to access a remote share, it copies itself there as NETMANAGER.EXE, and remotely executes itself as a service on the remote machine.
- Creates a share on the victim machine (share name "MEDIA").
- Mails itself, constructing message uses its own SMTP engine. E-mail attachment may be a ZIP archive. Mails are sent in reply to e-mail messages found on the victim machine. The subject line and message body of the e-mail vary.
- Renames the extensions of EXE files to ZMX.
- Terminates certain processes

This threat is written in the C++ programming language and is compressed with JDPack and ASPack.

W32.Netsky.S@mm (Alias: W32/Netsky.S@MM, Win32.Netsky.S, Worm Netsky.s, W32/Netsky-S) (W32 Worm): This mass-mailing worm, a variant of W32.Netsky.R@mm, contains backdoor functionality with the following characteristics:

- Constructs messages using its own SMTP engine.
- Harvests e-mail addresses from the victim machine.
- Spoofs the From: address of messages.
- Opens a port on the victim machine (TCP 6789).
- The attachment always will have a .pif file extension.
- Delivers a DoS attack on certain web sites upon a specific date condition between April 14 and 23, inclusive.

W32.Netsky.T@mm (Alias: WORM_NETSKY.T, W32/Netsky.t@MM, W32/Netsky-T, Win32.Netsky.T) (Win32 Worm): This mass-mailing worm, a variant of W32.Netsky.S@mm, contains backdoor functionality and may perform a Denial of Service (DoS) attack against specified Web sites. The e-mail has a variable subject line and attachment name. The attachment will have a .pif file extension.

W32.Randex.OL (Win32 Worm): This is a network-aware worm that spreads itself through shared network drives. It can receive instructions from an IRC channel on a specific IRC server. W32.Randex.OL may open ports 20, 113, 445, 1024, 55808, as well as randomly selected ports.

W32.Randex.PR (Alias: W32/Spybot.worm.gen.a) (Win32 Worm): This is a network-aware worm that attempts to copy itself to computers with weak administrator passwords. The worm receives instructions from an IRC channel on a predetermined IRC server.

W32.Sober.F@mm (Alias: W32/Sober.f@MM, Win32.Sober.F, W32/Sober-F, WORM_SOBER.F) (Win32 Worm): This variant of W32.Sober.E@mm spreads itself as an e-mail attachment, without destructive effects. The Subject: and Body: of the e-mail vary and are written in German or English.
Notes:

- The worm does not have a static MD5 hash value.
- The worm searches for e-mail addresses in files with several specific extensions, and then sends itself out to all the addresses it has gathered, using its own SMTP engine.

W32.Sober.F@mm is written in Microsoft Visual Basic and is packed with UPX.

W32.Solame.A (Alias: Exploit-Mydoom) (Win32 Worm): This worm spreads using the backdoor that the variants of W32.Mydoom@mm create.

WORM_AGOBOT.SY (Internet Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log on to systems using a predefined list of user names and passwords. It also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antiviral-related processes and dropped files by other malware. It also steals CD keys of certain game applications.

WORM_LOVGATE.U (Internet Worm): This memory-resident worm propagates through network shares using a list of common user names and weak passwords. It also uses MAPI to reply to messages found in a system. It attaches a copy of itself using several file names. It drops certain files with COM, EXE, PIF, and SCR extension names in the current folder and shared drives. It also terminates processes with certain strings.
This Aspack-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_NETSKY.R (Aliases: W32/Netsky.r@MM, W32.Netsky.R@mm) (Internet Worm): This worm uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate via e-mail. It gathers e-mail addresses from files with certain extension names in drives C to Z (except for CD-ROM drives). It also exploits a known vulnerability affecting Internet Explorer involving incorrect MIME Header (MS01-020), which allows the automatic execution of e-mail attachments while an e-mail is read or previewed. More information on this vulnerability is available at: http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx. The malware code reveals that this worm will launch a denial of service (DoS) attack against several Web sites beginning a specified date. It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_SPYBOT.JD (Alias: W32/Spybot.JD.worm) (Internet Worm): This memory-resident worm spreads via network shares. It accesses a system using a long list of common user names and weak passwords. It also has backdoor capabilities and connects to a specific Internet Relay Chat (IRC) server where it joins a particular channel using a random nickname. It then waits for several remote commands, which it processes on the machine. It also allows the remote user to launch flood attacks against a target Web site. This malware attempts to delete network shares using specific Windows NET.EXE commands. It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_SPYBOT.LJ (Internet Worm): This memory-resident worm spreads via network shares and Internet Relay Chat (IRC). It accesses a system using a long list of common user names and weak passwords. It connects to a specific Internet Relay Chat (IRC) server and joins a particular channel using a random nickname. It then waits for several remote commands, which it processes on the machine. It also allows the remote user to launch flood attacks against a target site. It also attempts to delete network shares using specific Windows NET.EXE commands. This malware arrives as an Exe32Pack compressed executable file and is written using Microsoft Visual C++, a high-level programming language. It runs on Windows 95, 98, ME, NT, 2000, and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Cazno	N/A	SB04-091
Backdoor.Cazno.Kit	N/A	SB04-091
Backdoor.Danton	N/A	SB04-091
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.IRC.Aimwin	**N/A**	**Current Issue**
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	L	CyberNotes-2004-05
Backdoor.IRC.Aladinz.M	M	CyberNotes-2004-05
Backdoor.IRC.Aladinz.N	**N**	**Current Issue**
Backdoor.IRC.Aladinz.O	**O**	**Current Issue**
Backdoor.IRC.Loonbot	N/A	CyberNotes-2004-05
Backdoor.IRC.Mutebot	**N/A**	**Current Issue**
Backdoor.IRC.MyPoo	N/A	SB04-091
Backdoor.IRC.MyPoo.Kit	N/A	SB04-091
Backdoor.IRC.Spybuzz	N/A	SB04-091
Backdoor.Kaitex.E	E	CyberNotes-2004-05
Backdoor.Medias	**N/A**	**Current Issue**
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.R3C.B	B	SB04-091
Backdoor.Ranky.E	E	SB04-091
Backdoor.Ranky.F	**F**	**Current Issue**
Backdoor.Sdbot.S	S	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tumag	N/A	SB04-091
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBH	N/A	CyberNotes-2004-01
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Download.Chamber	N/A	SB04-091
Download.Chamber.Kit	N/A	SB04-091
Download.SmallWeb	N/A	SB04-091
Download.SmallWeb.Kit	N/A	SB04-091
Download.Tagdoor	**N/A**	**Current Issue**
Downloader.Botten	N/A	CyberNotes-2004-05
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Downloader-IU	**IU**	**Current Issue**
Downloader.Psyme	**N/A**	**Current Issue**
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	N/A	CyberNotes-2004-05
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
MultiDropper-JW	JW	SB04-091
Needy.C	C	CyberNotes-2004-03
Needy.D	**D**	**Current Issue**
Needy.E	**E**	**Current Issue**
Needy.F	**F**	**Current Issue**
Needy.G	**G**	**Current Issue**
Needy.H	**H**	**Current Issue**
Needy.I	**I**	**Current Issue**
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	E	CyberNotes-2004-05
PWSteal.Bancos.F	F	SB04-091
PWSteal.Bancos.G	G	SB04-091
PWSteal.Banpaes.C	C	CyberNotes-2004-05
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Goldpay	**N/A**	**Current Issue**
PWSteal.Irftp	N/A	CyberNotes-2004-05
PWSteal.Lemir.G	**G**	**Current Issue**
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
PWSteal.Souljet	**N/A**	**Current Issue**
PWSteal.Tarno.B	B	CyberNotes-2004-05
PWSteal.Tarno.C	C	SB04-091
QReg-9	9	CyberNotes-2004-04
Spy-Peep	N/A	SB04-091
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Adtoda-A	**A**	**Current Issue**
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Badparty-A	A	SB04-091
Troj/Bdoor-CCK	CCK	CyberNotes-2004-05
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	D	CyberNotes-2004-05
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	A	CyberNotes-2004-05
Troj/Eyeveg-C	C	CyberNotes-2004-05
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	100	CyberNotes-2004-05
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/JDownL-A	**A**	**Current Issue**
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	G	CyberNotes-2004-05
Troj/LDPinch-H	H	CyberNotes-2004-05
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	A	CyberNotes-2004-05
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Prorat-D	D	SB04-091
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Ranckbot-A	A	SB04-091
Troj/Ranck-K	K	CyberNotes-2004-05
Troj/Rybot-A	**A**	**Current Issue**
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.AphexLace.Kit	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	F	CyberNotes-2004-05
Trojan.Bookmarker.G	G	SB04-091
Trojan.Brutecode	**N/A**	**Current Issue**
Trojan.Cookrar	**N/A**	**Current Issue**
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Dustbunny	N/A	SB04-091
Trojan.Etsur	N/A	CyberNotes-2004-05
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	N/A	CyberNotes-2004-05
Trojan.Gutta	N/A	CyberNotes-2004-04
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.KillAV.D	D	SB04-091
Trojan.Linst	N/A	SB04-091
Trojan.Lyndkrew	**N/A**	**Current Issue**
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	D	CyberNotes-2004-05
Trojan.Mitglieder.E	E	CyberNotes-2004-05
Trojan.Mitglieder.F	**F**	**Current Issue**
Trojan.Noupdate	N/A	CyberNotes-2004-05
Trojan.Noupdate.B	B	SB04-091
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Regsys	N/A	SB04-091
Trojan.Simcss.B	B	CyberNotes-2004-05
Trojan.Tilser	N/A	CyberNotes-2004-05
Trojan.Trunlow	**N/A**	**Current Issue**
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
W32.Tuoba.Trojan	N/A	SB04-091
Xombe	N/A	CyberNotes-2004-01

Backdoor.IRC.Aimwin: This Backdoor Trojan horse connects to Internet Relay Chat networks. This Trojan can also spread itself through the KaZaA file-sharing network, if the malicious user instructs it to do so.
Backdoor.IRC.Aladinz.N: This is a program that installs a Backdoor Trojan horse, which uses malicious scripts in mIRC client software, allowing for unauthorized remote access.

Backdoor.IRC.Aladinz.O: This is a Backdoor Trojan horse that uses malicious scripts in the mIRC client software, allowing for unauthorized remote access.

Backdoor.IRC.Mutebot (Alias: Backdoor.Loony.d, W32/Spybot.worm.gen.b): This Trojan horse has backdoor functionality, which allows a malicious user to control an infected computer via Internet Relay Chat (IRC).

Backdoor.Medias: This is a Trojan horse that installs itself as a Browser Helper Object.

Backdoor.Ranky.F: This Trojan horse runs as a proxy server. By default, the Trojan opens TCP port 54112.

Downloader-IU: This is a downloading Trojan known to have been spammed to many users in an e-mail bearing the following characteristics:

- From: support (support@the-body-shop.com) this may change
- Subject: Re: item purchase
- Attachment: DETAILS.ZIP (Zip file containing DETAILS.EXE)

The Trojan exists only to download and execute a remote file (path to which is stored in the Trojan). Access to the following domain should be blocked at the firewall to prevent the file download: http://marnet.us. When run, it attempts to download this file via HTTP, saving it to the Windows system directory as TEMPFILE.EXE:

- %SysDir%\TEMPFILE.EXE

This file is then executed. Obviously the exact contents of this file may change.

Downloader.Psyme (Alias: Troj/Psyme, VBS/Psyme, Trojan.VBS.KillAV): This Trojan horse downloads and executes a file. It uses a known exploit of ADODB stream objects in Microsoft Internet Explorer.

Download.Tagdoor: This is a group of Trojan horses that exploit the Internet Explorer Object Tag Vulnerability. (This is described in Microsoft Security Bulletin MS03-032.)

Needy.D (Alias: Java/Needy.D): Needy.D is a family of Java applet based Trojans that are downloaded into user computer and download further Trojans and modify explorer settings. Needy activates when user views a web page or HTML E-mail that contains reference to the Trojan. This variant of Needy, Needy.D is a simple Trojan downloader that downloads Trojan dropper win32.mute and executes it. It does not modify any settings by itself.

Needy.E (Alias: Java/Needy.E): This is a Java applet based Trojan that changes the Internet Explorer start page changes search settings to ones contained in the Trojan and downloads a Trojan downloader. Needy activates when user views a web page or HTML E-mail that contains reference to the Trojan file.

Needy.F (Alias: Java/Needy.F): This is a Java applet based Trojan that changes the Internet Explorer start page changes search settings to ones contained in the Trojan and downloads a Trojan downloader. Needy activates when user views a web page or HTML E-mail that contains reference to the Trojan file.

Needy.G (Alias: Java/Needy.G): This is a Java applet based Trojan that changes the Internet Explorer start page changes search settings to ones contained in the Trojan and downloads a Trojan downloader. Needy activates when user views a web page or HTML E-mail that contains reference to the Trojan file. Needy.G is otherwise identical to Needy.F except it downloads the instructions from a different address.

Needy.H (Alias: Java/Needy.H): This is a Java applet based Trojan that downloads and executes a Trojan downloader. Needy activates when user views a web page or HTML E-mail that contains a reference to the Trojan file.

Needy.I (Alias: Java/Needy.I): This is a Java applet based Trojan that changes the Internet Explorer start page, changes search settings to ones contained in the Trojan and writes shortcuts to pornographic services to users Internet Explorer link favorites.

PWSteal.Goldpay: This Trojan horse steals passwords, system, and personal information.

PWSteal.Lemir.G: This is a Trojan horse that attempts to steal the password of the "Legend of Mir 2" online game and send it to the malicious user.

PWSteal.Souljet: This Trojan horse steals system and personal information. The existence of the file spoo1sv.exe is an indication of a possible infection.

Troj/JDownL-A (Aliases: Trojan.Java.ClassLoader.c, Exploit-ByteVerify): This Trojan has been reported in the wild. It uses the Troj/ByteVeri-F exploit to download and install Troj/Banker-H.

Troj/Rybot-A (Alias: Backdoor.Rybot): This is a backdoor Trojan that allows a malicious user remote access to the computer via the IRC network. In order to run automatically when Windows starts up the Trojan copies itself to a user configurable filename and adds a registry run entry below:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run.

The Trojan also drops the files rplib.dll and rtm.dat in the Windows system folder. Troj/Rybot-A has the ability to log keystrokes and to send the logged data to a configurable FTP server.

Troj/Adtoda-A: This is a backdoor Trojan. When first run, the Trojan will display one of two messages. After the user clicks "OK" on both of these messages, Troj/Adtoda-A installs itself and activates the payload. This inverts the screen and freezes the machine so that is needs to be rebooted. In order to run automatically when Windows starts up the Trojan creates the file, C:\Windows\system\winupd32.exe and the shortcut, C:\Windows\Start Menu\Programs\StartUp\System Update Service.lnk pointing to it. These files will cause the payload to be run again on system boot. Troj/Adtoda-A also attempts to modify C:\boot.ini to prevent debugging.

Trojan.AphexLace.Kit: This Trojan encrypts an executable and appends it to the end of another unencrypted executable.

Trojan.Brutecode: This is a Trojan horse that modifies various registry keys.

Trojan.Cookrar: This is a Trojan horse that takes screenshots of login Web pages, and then e-mails them to a remote server. When Trojan.Cookrar is executed, it looks for Internet Explorer windows that are open with URLs containing:

- https:/ /ibank.barclays.co.uk/fp/1_2d/online

Trojan.Lyndkrew: This Trojan horse deletes critical files.

Trojan.Mitglieder.F (Alias: W32/Bagle.gen@MM, TrojanProxy.Win32.Mitglieder.ag, WORM_BAGLE.W): This variant of Trojan.Mitglieder opens a proxy on the system, attempts to stop security software, and can update itself.

Trojan.Trunlow (Aliases: Troj/Psyme, VBS/Psyme, Trojan.VBS.KillAV, Trojan Horse, Downloader.Trojan): This is Trojan horse that attempts to steal passwords, including cached Windows passwords, protected storage passwords, and passwords for dial-up accounts and mail accounts. This Trojan is usually distributed through links hidden in web pages or pop-up windows, and may exploit Internet Explorer vulnerabilities to download and execute files.